

## UNITED STATES DISTRICT COURT

for the  
Western District of OklahomaAMG  
8/22/23In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)ELECTRONIC DEVICES: A GRAY TCL CRICKET FLIP PHONE, WITH ASSIGNED  
PHONE NUMBER OF (405) 900-3202, AND A BLACK MOTOROLA SMART PHONE,  
WITH ASSIGNED PHONE NUMBER OF (405) 500-9419, WHICH ARE CURRENTLY  
LOCATED AT 3625 NW 56TH STREET, OKLAHOMA CITY, OK 73112

Case No. MJ-23- 648-AMG

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached and incorporated by reference.

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.


The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251(a) & (e)	Attempted sexual exploitation of a child
18 U.S.C. § 1470	Attempted transfer of obscene material to a minor
18 U.S.C. § 2260A	Commission of a felony sex offense by an individual required to register as a sex offender
18 U.S.C. §§ 2252A(a)(2)(A) & (b)(1)	Distribution and attempted distribution of child pornography

The application is based on these facts:

See attached Affidavit of HSI Special Agent Scott Muncaster, which is incorporated by reference herein.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

 Scott Muncaster, SA, HSI  
 Printed name and title

Sworn to before me and signed in my presence.

Date:

8/22/23

  
 Judge's signature

City and state: Oklahoma City, Oklahoma

 AMANDA MAXFIELD GREEN, U.S. MAGISTRATE JUDGE  
 Printed name and title

**IN THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF OKLAHOMA**

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Scott Muncaster, a Special Agent with the Department of Homeland Security, Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI) since May 2017, and I am currently assigned to the office of the Resident Agent in Charge, Oklahoma City. I am also an investigative member of the Oklahoma Internet Crimes Against Children (OK ICAC) taskforce. While employed by HSI, I have been involved in investigations of child exploitation matters and computer crimes against children. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as a Special Agent with HSI.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Matthew Ryan STROBL, a currently registered sex offender in the State of Oklahoma. On or about August 16, 2023, STROBL was indicted by a federal grand jury in the Western District of Oklahoma for Attempted Sexual Exploitation of a Child in violation of 18 U.S.C. § 2251(a) and (e); Attempted Transfer of Obscene Material to a Minor in violation of 18 U.S.C. § 1470;

Commission of a Felony Sex Offense by an Individual Required to Register as a Sex Offender in violation of 18 U.S.C. § 2260A; and Distribution and Attempted Distribution of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (“the SUBJECT OFFENSES”).

4. This Affidavit seeks authorization to search: (1) STROBL’s gray TCL Cricket flip phone, with assigned phone number of (405) 900-3202, further described in Attachment A, and (2) STROBL’s black Motorola smart phone, with assigned phone number of (405) 500-9419, further described in Attachment A, collectively referred to as the “SUBJECT DEVICES,” to seize therefrom the items described in Attachment B, which constitute instrumentalities, fruits, and evidence of STROBL’s violations of the SUBJECT OFFENSES.

5. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

6. The SUBJECT DEVICES are currently secured at the HSI, Resident Agent in Charge, Oklahoma City, Oklahoma forensic lab, located at 3625 NW 56<sup>th</sup> Street, Oklahoma City, Oklahoma 73112. As set forth below, there is probable cause to believe that STROBL possessed, owned, and used the SUBJECT DEVICES to commit the SUBJECT OFFENSES.

7. The facts in this Affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents. Since

this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

8. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

9. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

10. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications, as well as applications like Instagram. Additionally, individuals utilize their cellular devices to take and store pictures and keep

notes. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual.

11. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during, and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the SUBJECT OFFENSES, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ

techniques (including but not limited to computer-assisted scans of the entire medium) that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause to authorize execution of the warrant at any time in the day or night.

15. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the SUBJECT DEVICES. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in



their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

### **TECHNICAL TERMS**

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. “Computer” refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, “computer” also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. *See* 18 U.S.C. § 1030(e)(1).
- b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers



in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- c. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- d. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash

memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to

access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I believe that at least one of the SUBJECT DEVICES, the black Motorola smart phone, has capabilities that allow it to serve as a wireless telephone, computer, digital camera, portable media player, GPS navigation device, and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **STATEMENT OF PROBABLE CAUSE**

18. In March 2023, an HSI Special Agent (“the UCA”) tasked with conducting Online Child Exploitation investigations was acting in an undercover capacity as a juvenile female on various social media and messaging platforms, including Instagram.

19. On or about March 20, 2023, the UCA’s undercover Instagram profile received notification that Instagram user “therabbitt08” sent a message to the UCA profile. The UCA observed that the Instagram profile picture associated to “therabbitt08” depicted two confederate flags, side-by-side, with the words “Southern Pride” in text across the picture.<sup>1</sup>

20. In initiating contact with the UCA, “therabbitt08” stated, “U are so beautiful and sexy.” After the UCA’s response thanking “therabbitt08,” he said, “You’re welcome love,” followed by “How old are you?”, upon which the UCA responded, “14” and “U”. “therabbitt08” responded, “I’m 33” and “That ok with you?” As the conversation

---

<sup>1</sup> Within the direct messaging screen of the Instagram chat between the UCA and “therabbitt08,” the UCA could see that the Instagram profile “therabbitt08” was identified by screen name “Matt.”

continued, the UCA advised “therabbitt08” that they lived in Arizona, and “therabbitt08” responded that he lived in Oklahoma.

21. The UCA asked “therabbitt08” (later identified as STROBL) if he ever came to Arizona. STROBL responded, “No but for u I would” “to meet you that is.” The UCA responded, “I hear that a lot.” STROBL replied, “Lol I bet” and “U are so sexy.” After additional back-and-forth, STROBL asked the UCA if she has a boyfriend, upon which the UCA stated that she did not. STROBL replied, “I wish I could by your boyfriend”. The UCA then asked STROBL what he looked like, upon which he replied, “Ugly.” After STROBL’s reply, the UCA received several “selfie” pictures of a male subject that were later determined to match the physical description of STROBL.

22. The UCA responded to the “selfie” photos sent by STROBL with flame emojis, and STROBL responded, “Really?” “U think so?” The UCA replied, “Def.” And then STROBL replied, “Awesome” “I’m glad” “Would u wanna meet me?” The UCA replied, “Definitely” “To bad your in Oklahoma” upon which STROBL replied, “Yeah I know” “What would we do if we met?”

23. As the conversation continued, STROBL inquired about doing things with the UCA with her clothes off and eventually inquired if the UCA would have sex with him if they were together. STROBL then sent a cartoon picture of a man performing oral sex on a female. The caption reads, “after work n before work should be like dis”.

24. Throughout the ongoing conversation between the UCA and STROBL, STROBL inquired as to whether or not the UCA is a virgin and discussed topics of a sexual

nature. STROBL also asked the UCA if she could send him “sexy pics.” However, the UCA replied that she does not send “pics like that.” The UCA then sent STROBL a phone number to contact her via text message and explained that her mom does not like her to be on “insta” all night. On that same date, the UCA received a text message from phone number (405) 900-3202.

25. The UCA conducted record checks of phone number (405) 900-3202 via law enforcement database queries. The records checks revealed that the phone number was associated to Matthew STROBL with DOB: 09/07/19XX and an Oklahoma City, Oklahoma address.

26. Additional records checks for STROBL revealed that he is a currently registered sex offender in the State of Oklahoma and is currently on supervised release, under the supervision of the Oklahoma Department of Corrections, Probation and Parole Division.

27. Throughout the various conversations between the UCA and STROBL, STROBL continued to ask for photographs of a sexual nature from the UCA and discussed a willingness to have sex with the UCA. Within these chat conversations, STROBL also sent digital images of an erect penis and videos depicting an adult male masturbating into a bathroom sink.

28. In June 2023, STROBL sent the UCA internet links, via Instagram, that provided access to Mega and Dropbox online cloud-based server platforms. The links contained numerous digital photograph and video files that, after review, are believed to

be child pornography, some examples of which depict pre-pubescent females performing oral sex on what appear to be unknown adult males; fully nude pre-pubescent females and males that appear to be approximately 5-to-10 years of age performing sexual acts on each other; and unknown adult male subjects having vaginal and anal sexual intercourse with female toddlers and infants.

29. Further, STROBL described some of the image files he sent to the UCA as being of a 13-year-old female, from the “UK”, that he also communicates with. STROBL then stated, via text message to the UCA, that the poses in the pictures of the juvenile female he sent the UCA are ideas for how he wants the UCA to pose in pictures to him. STROBL had, prior to sending these pictures, requested that the UCA send STROBL pictures of herself on numerous occasions.

30. On June 12, 2023, Department of Homeland Security (DHS) Administrative Summons #HSI-NG-2023-114216 was served to AT&T Corporation to produce subscriber information for phone number (405) 900-3202. AT&T responded that the phone number was associated to AT&T-affiliated Cricket, and that the “Financial Liable Party” for the phone number is Elizabeth Okoluk at a specific address in Edmond, Oklahoma with Activation Date of August 8, 2022. According to Oklahoma Department of Corrections records, Elizabeth Okoluk is listed as STROBL’s fiancé. Additionally, AT&T responded that the account number associated to (405) 900-3202 is #431851558, and that the “Billing Party” for the account is Matthew STROBL of the same Edmond, Oklahoma address. AT&T also provided that the international mobile subscriber identity



(IMSI) associated to the phone number is 310150753089972.

31. On June 23, 2023, an HSI Oklahoma City Special Agent contacted the Oklahoma Department of Corrections, Probation and Parole Division (OK DOC) and spoke with STROBL's assigned probation officer, Steven Riha. Officer Riha advised that STROBL is in fact currently under OK DOC supervision, is a currently registered sex offender, is classified as "transient" by OK DOC, and was scheduled to report to the OK DOC on Monday, June 26, 2023, for a weekly scheduled check-in. Officer Riha also advised the HSI Special Agent that, due to his current sex offender status, STROBL is currently on an "Internet Safety Plan," which is intended to restrict his access to the internet and social media. Additionally, as a condition of STROBL's supervised release and sex offender status, he and any electronic device in his possession is subject to search by OK DOC personnel. HSI asked Officer Riha what phone number STROBL uses to communicate with OK DOC. Officer Riha responded that STROBL's number that he communicates with OK DOC is (405) 900-3202.

32. On June 25, 2023, the UCA again received text messages from STROBL requesting that the UCA take photographs of herself and send them to him. STROBL then sent approximately 15 digital images to the UCA as a guide for how the UCA should pose in the pictures, some examples of which include: a photo of a female with her breasts exposed; a nude female bent over a bed exposing her vagina and buttocks; a nude female exposing her vagina and anus simulating masturbation; and a close-up photo of exposed anus and vagina being spread by two fingers.

33. On Monday, June 26, 2023, STROBL reported to the OK DOC office located at 1501 N. Classen Blvd., Oklahoma City, Oklahoma 73106 as scheduled. During the appointment, Officer Riha took possession of the black Motorola Cricket cellular phone that STROBL brought to the appointment in order to conduct a search of the device ("Phone 1"). While Officer Riha was searching Phone 1, the UCA sent a text message to STROBL to confirm that Phone 1 was the device STROBL was using to communicate with the UCA. As Officer Riha observed, Phone 1 received the text message from the UCA.

34. After observing violations of STROBL's probation conditions, Officer Riha confiscated Phone 1, and HSI obtained a search warrant for the device.

35. Following Officer Riha's confiscation of Phone 1, STROBL continued to communicate with the UCA sporadically using phone number (405) 900-3202 until on or about July 4, 2023. Based on my training and experience, I believe that after having his first cell phone confiscated by OK DOC, STROBL purchased a new cellular phone and had the (405) 900-3202 number assigned to the new phone ("Phone 2"). I know that a person who loses a cell phone can go to their respective cell phone retailer to purchase a new phone and request their original number be assigned to the new phone.

36. On or about July 4, 2023, the UCA received a text message from STROBL from a new phone number: (405) 500-9419. STROBL stated that his other phone was about to be "shut off." STROBL stated to the UCA that his new phone ("Phone 3") was a smart phone, whereas the phone he was previously communicating with her on (Phone 2) was a flip phone.

37. In the conversations between the UCA and STROBL in which STROBL utilized Phone 3, STROBL again asked the UCA for pictures. Additionally, STROBL sent the UCA pictures of an adult female posing with her genitals exposed. STROBL also sent pictures of himself to the UCA.

38. Finally, on or around July 5, 2023, HSI obtained a search warrant for STROBL's Instagram account: "therabbitt08". Review of the production provided by Instagram revealed that STROBL has sent child pornography via Instagram to other individuals on various occasions. For example, on or around April 5, 2023, STROBL sent a 24-second video of what appears to be a prepubescent female performing oral sex on an adult male to username lilysome\_one. I thus believe STROBL has distributed child pornography to others in addition to the UCA.

39. After STROBL was indicted, on or about August 18, 2023, he was arrested pursuant to an arrest warrant after he arrived at the OK DOC office for an appointment with Officer Riha. When STROBL was arrested, he had a gray TCL Cricket flip phone in his pocket, one of the SUBJECT DEVICES. Since STROBL has previously described Phone 2 as a flip phone and this phone is a flip phone, I believe that this phone is Phone 2, one of the devices STROBL used to communicate with the UCA.

40. When STROBL arrived for his appointment with Officer Riha, he arrived in a car driven by a driver affiliated with the nonprofit organization providing housing for STROBL. After STROBL was arrested, law enforcement approached the vehicle, with the driver inside, to ask if STROBL had any additional personal property in the vehicle. The

driver pointed to a backpack in the passenger seat of the vehicle. Agents seized the backpack, which STROBL later confirmed belonged to him. While speaking with the driver through the driver's side window, an agent noticed what appeared to be a cell phone in the passenger door pocket of the door of the vehicle. Agents pulled the phone out of the door pocket to show it to the driver and asked the driver if the cell phone belonged to him, and he stated he didn't know anything about the cell phone. I then asked the driver to confirm if it belonged to him or not, and he stated it did not belong to him, and he showed me his own cell phone. I called the phone number associated with Phone 3, and the cell phone found in the door pocket rang. STROBL denied that this device, one of the other SUBJECT DEVICES, belonged to him.

41. Based on the above, there is probable cause to believe that evidence of STROBL's violations of the SUBJECT OFFENSES will be found on the SUBJECT DEVICES.

#### **BIOMETRIC ACCESS**

42. The warrant I am applying for would permit law enforcement to obtain from STROBL the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock the SUBJECT DEVICES pursuant to this warrant. I seek this authority based on the following:

43. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to

unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

44. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

45. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

46. In my training and experience, users of electronic devices often enable the

aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

47. As discussed in this affidavit, HSI has seized the two SUBJECT DEVICES, one of which is a smart phone. Any passcode or password that would unlock the SUBJECT DEVICES is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

48. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the

device through a biometric feature may exist for only a short time.

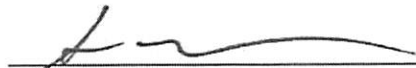
49. Due to the foregoing, if either of the SUBJECT DEVICES may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of STROBL, who is reasonably believed by law enforcement to be a user of the SUBJECT DEVICES, to the fingerprint scanner of either device; (2) hold either device in front of the face of STROBL and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

#### **CONCLUSION**

50. Based on the foregoing, there is probable cause to believe that the SUBJECT OFFENSES have been committed, and that contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT DEVICES. I respectfully request that this Court issue a search warrant authorizing the search of the SUBJECT DEVICES described in Attachment A to seize the items described in Attachment B.

**[CONTINUED ON THE FOLLOWING PAGE]**





Scott Muncaster  
Special Agent  
Homeland Security Investigations

SUBSCRIBED AND SWORN to before me this 22<sup>nd</sup> day of August, 2023.



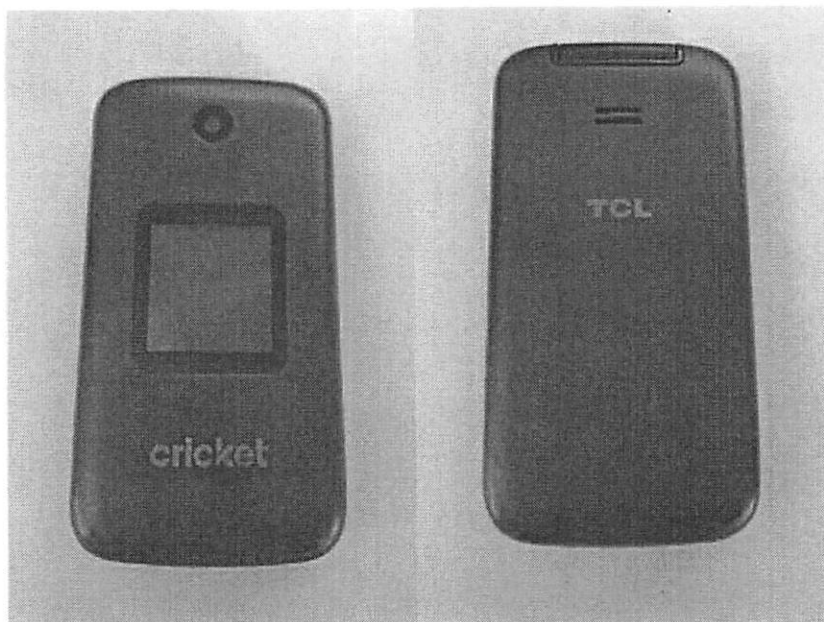
AMANDA MAXFIELD GREEN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

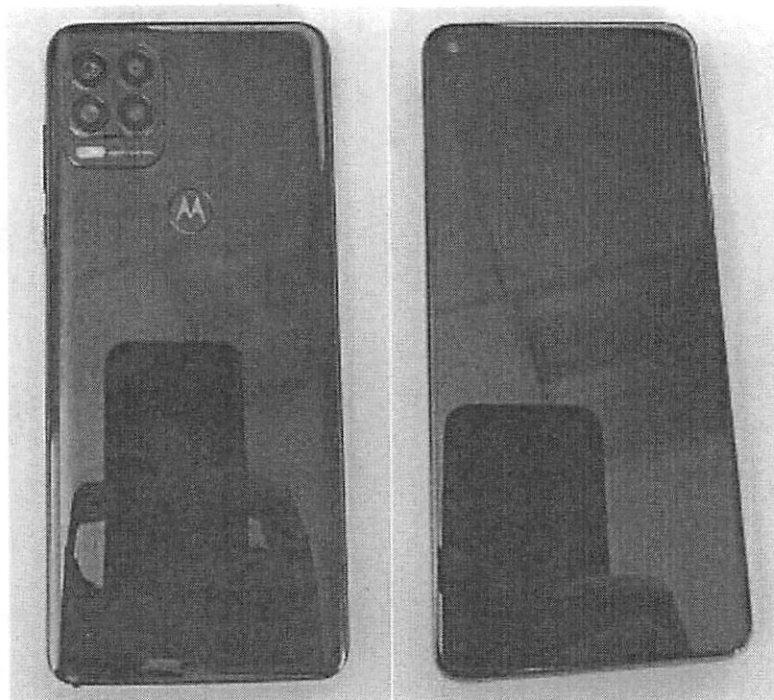
This warrant seeks to search:

- STROBL's gray TCL Cricket flip phone, with assigned phone number of (405) 900-3202, which is currently secured at HSI, Resident Agent in Charge, Oklahoma City, Oklahoma forensic lab, located at 3625 NW 56<sup>th</sup> Street, Oklahoma City, Oklahoma 73112, and is depicted below:



[CONTINUED ON THE FOLLOWING PAGE]

- STROBL's black Motorola smart phone, with assigned phone number of (405) 500-9419, which is currently secured at HSI, Resident Agent in Charge, Oklahoma City, Oklahoma forensic lab, located at 3625 NW 56<sup>th</sup> Street, Oklahoma City, Oklahoma 73112, and is depicted below:



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

All records on the SUBJECT DEVICES described in Attachment A that relate to violations of the SUBJECT OFFENSES (Attempted Sexual Exploitation of a Child in violation of 18 U.S.C. § 2251(a) and (e); Attempted Transfer of Obscene Material to a Minor in violation of 18 U.S.C. § 1470; Commission of a Felony Sex Offense by an Individual Required to Register as a Sex Offender in violation of 18 U.S.C. § 2260A; and Distribution and Attempted Distribution of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1)), including:

**I. Digital Evidence**

1. Any passwords, password files, test keys, encryption codes, or other information necessary to access the SUBJECT DEVICES;
2. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device described in Attachment A, that show the actual user(s) of the computer or digital device during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the device; MAC IDs and/or Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; software that would allow others to control the digital device such as viruses, Trojan horses, and other

forms of malicious software; evidence of the absence of such malicious software, or of the presence or absence of security software designed to detect malicious software;

3. Evidence that the device was attached to or used as a data storage device for some other device, or that another device was attached to the device; and

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device;

## **II. Records, Documents, and Visual Depictions**

5. Any records, documents, or materials, including correspondence, that pertain to any conversations with the Undercover Agent (UCA) described in the affidavit in support of the search warrant application in any form including Instagram, text message, or any other social media platform;

6. Any records, documents, or materials, including correspondence, that involve any communication with any person that appear to be coercive in nature for the purposes of grooming or obtaining images from any person;

7. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

8. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

9. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

10. Any records, documents, or materials, including correspondence, which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

11. Any records, documents, or materials, including correspondence, relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

12. Any records, documents, or materials, including correspondence, naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

13. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet on any app installed on the SUBJECT DEVICES;

14. Any records, documents, or materials, including correspondence, referring or pertaining to communications with others, whether in person, by telephone, or online,

for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received;

15. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and/or notes associated with child pornography or those who collect, disseminate, or trade in child pornography; and

16. Any records, documents, materials, videos, conversations, or photographs that would allow investigators to ascertain who used the SUBJECT DEVICES.

As used above, the terms records, documents, programs, applications, or materials includes records, documents, programs, applications or materials created, modified, or stored in any form, including digital or electronic form.

During the execution of the search of the SUBJECT DEVICES described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Matthew Ryan Strobl to the fingerprint scanner of the device; and (2) hold the device in front of the face Matthew Ryan Strobl and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Matthew Ryan Strobl is a white male with a date of birth of 09/07/19XX and is depicted on the following page:

**[CONTINUED ON THE FOLLOWING PAGE]**



